Virginia Information Technologies Agency

Commonwealth Information Security Council
Risk Management Committee Meeting

May 17, 2010
2:00-3:00 pm CESC

Risk Management Committee members attending:

Joshua Cole, DOAV *
Ed Miller, Co-Chair
Aaron Mathes, OAG, Co-Chair *
Ross McDonald, DSS
John Spooner, DOA *
Jeremy Greenwood, TRS
Bob Auton, DJJ *

* (Teleconference to CESC)

Risk Management Committee members absent:

Goran Gustavsson, APA, Co-Chair *
Mauri Shaw, CSRM

Also Attending:

John Green, COV CISO
Benny Ambler, CSRM
Aarona Brooks, CRSM
Carsten Schmidt, IREC*

Topic: Risk Management - Discussion of the IREC Diagnostic Tool via GoTo Meeting

- Diagnostic Description: This Tool helps (1). Benchmark against peers, (2). Target areas for improvement, and (3). Accelerate performance.

- The Diagnostic Tool is composed of 25 competencies. The competencies can have different levels of importance and effectiveness that are rated on a scale of 1 – 5.

- The Diagnostic Tool is composed of six categories: (1). Strategy and Planning, (2). Architecture Design and Implementation, (3). Awareness and Training, (4). Operational Maintenance and Control, (5). Cross-functional Collaboration, and (6). Performance Management and Value.

- John asked Carsten how the results of the Diagnostic Tool relate to the Risk Management framework. Carsten mentioned that the Diagnostic Tool helps identify what everyone thinks is key, what competencies everyone should have, it helps define and build the program, and helps identify the biggest skill gaps.

- John mentioned that the Diagnostic Tool will need to operate at the Commonwealth-level, as well as the Agency-level. For instance, one Agency

might have requirements that the Agency is not able to meet due to financial constraints. However, if the same significant risk existed for many other Agencies and as a result, gaps needed to be mitigated, then the data gathered from the Diagnostic Tool might be presented to the General Assembly to help demonstrate the need for funding to help mitigate these risks. John envisions the Diagnostic Tool being used to help explain information security risks and show the need for funding to mitigate risks at the Commonwealth-wide level.

- Aaron asked about deliverables. Aaron mentioned that Agencies currently, and will continue to assess their own information security risks in the future. Also, as transformation continues, a risk could be this or that. Aaron mentioned that there could be two layers of risks: (1). Four or five Agencies could have the same risk(s), and (2) Northrop Grumman could be an international target.

- John mentioned that he does not expect reporting requirements to go above and beyond what Agencies are already reporting for their Information Security program.

- Ed mentioned that the Diagnostic Tool will provide a method to prioritize risks and that the Tool could be used as a template.

Going forward with action plan:

- Carsten Schmidt will send John Green a link to the Diagnostic Tool.

- John will send the Diagnostic Tool's link to committee members for everyone to test within one week. As the committee members complete and answer the IREC Diagnostic Tool, the answers should address the broader Commonwealth's needs versus the needs of any one particular Agency.

- After 3 – 4 business days, Carsten will review the results and provide feedback, summarizing the information for John.

- IREC will put together an analysis and schedule a conversation to review the results with John prior to the next Council/Committee meeting.